## REMARKS

**Status**:

Claims 1-3 stand finally rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. And, claims 1-12 stand finally rejected under 35 U.S.C. §103(a) as being unpatentable over the teaching of U. S. Pat. No. 5,923,756 to Shambroom, considered with the teaching of Schneier in "Applied Cryptography" in view of the teaching of Balenson, " Privacy Enhancement for Internet Electronic Mail: Algorithms, Modes, and Identifiers", Network Working Group, Request For Comments (RFC) 1423, February 1993.

Claims 1-12 as amended are presented for reconsideration as explained in the analysis that follows.

**Analysis:**

Claim 1 has been amended to clarify the subject matter of claims 1-3 as being structure for functioning in a computer apparatus. It is believed this satisfies 35 U.S.C. §101 and a withdrawal of the rejection based thereon is respectfully solicited.

As regards X.509 certificates, Attachment A of Applicant's previous amendment (hereinafter "Standard") spells out the profile that is dictated by the relevant standards organization. Section 4.1 of the Standard specifies the content of the basic certificate fields. At Section 4.1.2.7 there is provision for only one public key and one algorithm associated with that key.

Now looking to the Schneier teaching at Fig.24.2, it appears to be a graphic representation of the X.507 certificate profile without any extensions. There is one public key associated with one cryptographic algorithm (see Subjects Public Key box). This teaches or suggests nothing beyond the original standard without provision for extensions.

Shambroom at col. 10, line 33-35 mentions listing of algorithms supported by the server and a certificate resembling an X.507 certificate; but, gives no further detail. Where does Shambroom indicate that the certificate would actually allow a device to authenticate for an alternate listed algorithm? And, more importantly, where does he explain how to do so within the constraints of the Standard? The Standard provides for identification of one public key and one associated algorithm (Section 4.1.2.7)..

Applicant recognized the desirability of complying with the Standard while achieving algorithm flexibility not intended by the Standard. Moreover, Applicant stretched the Standard to support legacy devices while providing new alternatives for devices capable of working with Applicant's special extensions. These are compliant extensions, but, extensions serving a purpose not suggested or recommended by the Standard.

Balenson teaches the need for improved algorithms in view of security problems. But, there is no suggestion of providing for alternative algorithms under the current Standard. Where is there a suggestion for more than one public key in a certificate, let alone, a fix to provide such with the current X.507 v.3 certificate profile?

The claims have been amended to emphasize multiple public keys with associated algorithms. As claimed, the added public key(s) are specified and certified in certificate extensions (see claim 1, lines 5-10) as is nowhere taught or suggested in the prior art. Compare Schneier's Fig. 24.2 which doesn't even show extensions.

In accordance with the foregoing, it is believed that the subject Application clearly identifies inventive subject matter not taught or suggested in the prior art. Hence Applicant respectfully solicits withdrawal of the rejection of claims under 35 U.S.C. §103(a) and early notice that this case has been placed in condition for allowance.

Respectfully Submitted,

George E. Grosser

Reg. No. 25,629l

c/o IBM Corp.
Dept. T81/Bldg. 503 PO Box 12195
Research Triangle Park, NC 27709
(919)968-7847 Fax 919-254-4330
EMAIL: gegch@prodigy.net